Nationale Initiative für Internet-Sicherheit

advice
Ausgabe 01/2007

Liebe NIFIS-Mitglieder,
sehr geehrte Interessenten und Förderer,

unser junger Verein wird von der Politik, der Wirtschaft und anderen Organisationen im Bereich Sicherheit als kompetenter und zuverlässiger Partner wahrgenommen. Wir sind beteiligt an den Diskussionen zur Umsetzung des Nationalen Plans zum Schutz von Informationsinfrastrukturen (NPSI). NIFIS wurde um Stellungnahme gebeten zur Frage, ob Kommunalwahlen in Hessen künftig online möglich sein sollen. Unser Sicherheitsreport, den wir Ihnen in dieser Ausgabe von NIFIS advice vorstellen, fand große Beachtung in Fachkreisen und der Presse. Auf unserer Website stellen wir laufend wichtige Informationen und aktuelle Warnhinweise bereit. Außerdem haben wir eine weit reichende Kooperation mit der COMPUTERWOCHE geschlossen, um deutsche Unternehmen noch stärker für das Thema IT-Sicherheit zu sensibilisieren. Bei NIFIS tut sich also Einiges!

Allerdings nutzen noch zu wenige Mitglieder die Chancen, die NIFIS als Plattform bietet. Als zentrale Anlaufstelle beantworten Experten interdisziplinär und neutral Fragen rund um die Internet-Sicherheit. Profitieren Sie von den vielfältigen Informationen, Dienstleistungen und praxisnahen Hilfestellungen, damit Ihr Unternehmen bestens geschützt ist. Gestalten Sie die Entwicklung Ihres Vereins aktiv mit, indem Sie beispielsweise unter Hinweis auf NIFIS auf andere zugehen, um diese auf das Thema Internet-Sicherheit anzusprechen. Dies bedeutet eine Win-Win-Situation, da NIFIS als neutrale Institution die Tür öffnet, und gleichzeitig die Möglichkeit besteht, neue Mitglieder für NIFIS zu gewinnen. Also: Nutzen Sie NIFIS, und nützen Sie ihr damit!

Viel Spaß beim Lesen wünscht Ihnen

Thomas Lapp, Vorstand der NIFIS

HIGHLIGHTS

NIFIS-Sicherheitsreport

Der größte Schaden nach einem Sicherheitsvorfall in IT-Systemen liegt für Unternehmen im Verlust geschäftskritischer Daten. Das sagen 82 Prozent der im Rahmen einer empirischen Erhebung von NIFIS befragten 100 Branchenkenner. „Ein interessantes Resultat der Umfrage ist, dass auf die Frage, ob der unmittelbare Verlust von Geld das größte Problem darstellt, immerhin ein Fünftel mit ‚Nein' geantwortet hat", erläutert NIFIS-Vorstandsvorsitzender Peter Knapp.

Hinter dem Verlust geschäftskritischer Daten folgt an zweiter Stelle mit 72 Prozent der Stimmen die lange Ausfallzeit produktiver Systeme. 52 Prozent der Fachleute sehen darüber hinaus im Imageverlust ein besonderes Problem. „Vorausgesetzt, ein Sicherheitsvorfall wird in der Öffentlichkeit bekannt, kann der Folgeschaden infolge von Kündigungen seitens bestehender Kunden und fehlender neuer Geschäftsabschlüsse sogar liquiditätsbedrohend sein", kommentiert Knapp. ►

63 Prozent der Befragten haben im Jahr 2006 im eigenen oder in einem bekannten Unternehmen von Problemen im Zusammenhang mit der Informations-Sicherheit gehört.

Wie die Umfrage ergab, ist eine der größten Gefahren für die Informations-Sicherheit eines Unternehmens der eigene Mitarbeiter, der unbewusst nachlässig mit Passwörtern umgeht oder etwa mobile Speicher auf unerlaubte Weise nutzt.

72 Prozent der Befragten sehen eine große Bedrohung der Firmendaten durch Viren, Würmer und Trojanische Pferde. 28 Prozent waren der Ansicht, das Hauptproblem im Zusammenhang mit Lücken in der Informations-Sicherheit seien zu lockere Security Policies.

NIFIS vertritt zwar die Meinung, dass das Sicherheitsbewusstsein in deutschen Unternehmen gestiegen ist, dennoch werde dem Thema Informations-Sicherheit gerade im Hinblick auf eine kontinuierliche und langfristige Datenabsicherung immer noch nicht der Stellenwert eingeräumt, der eigentlich notwendig ist. ►

38 Prozent der Branchenkenner sehen in der nicht ausreichenden Pflege und Wartung bestehender Systeme einen Hauptgrund für Sicherheitsprobleme. „Das hängt damit zusammen, dass mittlerweile zwar die meisten Unternehmen Sicherheitslösungen implementieren, dann aber glauben, damit sei alles für die Informations-Sicherheit getan. Diese lässt sich aber nicht durch eine einmalige Aktion herstellen, sondern nur über einen kontinuierlichen Prozess, der stetige Aufmerksamkeit verlangt und weiterentwickelt werden muss“, erklärt Knapp.

Laut Umfrage schätzen die Experten, dass Unternehmen in Deutschland bis 2011 ihre Ausgaben für die Informations-Sicherheit deutlich erhöhen werden. Um diese langfristig und kontinuierlich zu stabilisieren, stehen bei den Unternehmen nach Einschätzung der Befragten die Aufklärung und Schulung von Mitarbeitern sowie die Etablierung einer unternehmensweiten Security Policy mit entsprechenden Verhaltensregeln im Fokus. ❑

NIFIS rät zu IDM-System

Um das Niveau ihrer Datensicherheit zu erhöhen, empfiehlt NIFIS Unternehmen dringend die Einführung eines Identity-Management-Systems (IDM). Dieses entspreche nicht nur den höheren Anforderungen aus den gesetzlichen Vorschriften, sondern helfe, massiv Kosten einzusparen.

„Die Verwaltung der Zugriffsrechte ist heute eine gewaltige Herausforderung für ein Unternehmen – dies umso mehr, wenn es über Niederlassungen in der ganzen Welt und eine entsprechend hohe Mitarbeiterzahl verfügt“, sagt NIFIS-Vorstand Thomas Lapp. Ohne zentrales System, das die Vielzahl der Kennungen und personenbezogenen Informationen reduziert, die Anwender für den Zugriff auf die Applikationen und Datenbestände brauchen, ist diese Herausforderung nicht mehr zu stemmen. Außerdem besteht aufgrund zahlreicher neuer Vorschriften wie Basel II, dem Bilanzrechtsreformgesetz und dem Gesetz zur Unternehmensintegrität akuter Handlungsbedarf. ►

„Zwar verlangt keine Vorschrift direkt die Einführung eines IDM-Systems, doch müssen Unternehmen in der Lage sein, zu jeder Zeit Auskunft darüber zu geben, welche Mitarbeiter Zugriff auf geschäftskritische Daten, beispielsweise in Zusammenhang mit der Bilanzierung, hatten“, so Lapp. Weitere Informationen finden Sie auch im Artikel zu unserem IM-Kompetenzzentrum sowie im aktuellen Praxistipp. ❑

Institut für System-Management erhält NIFIS-Siegel

Das Institut für System-Management hat den umfassenden Sicherheitscheck bestanden und darf nun für zwölf Monate das NIFIS-Siegel führen. Dieses belegt den hohen Sicherheitsstandard gegenüber Mitarbeitern, Kunden und Geschäftspartnern.

Vorausgegangen war der Erteilung eine umfangreiche Selbstanalyse des Institutes für System-Management, bei der 82 Fragen aus den Bereichen organisatorische, logische, technische sowie physikalische Sicherheit beantwortet wurden.

Der NIFIS-Siegelrat hat diese Antworten analysiert und dem Unternehmen bestätigt, dass für den Bereich Informationstechnologie sehr gute Vorkehrungen zum Schutz vor Gefahren aus dem Internet und vor Risiken in der IT getroffen wurden.

Das NIFIS-Siegel wurde speziell für die mittelständische Wirtschaft entwickelt und ist die erste Stufe im Prozess zur Vorbereitung einer Zertifizierung gemäß ISO 27001. Für NIFIS-Mitglieder ist der Erwerb des Siegels **kostenfrei** möglich, Nicht-Mitglieder zahlen 150 Euro.

Prüfen und optimieren Sie jetzt Ihren Schutz vor Gefahren aus dem Internet! Schreiben Sie bei Interesse eine E-Mail an newsletter@nifis.de.

Weitere Informationen erhalten Sie hier. ❑

COMPUTERWOCHE und NIFIS kooperieren

Um einen direkten Beitrag zur Steigerung des IT-Sicherheitsniveaus zu leisten, haben COMPUTERWOCHE und NIFIS eine weit reichende Kooperation geschlossen. Beide Partner wollen sich gemeinsam dafür einsetzen, Unternehmen in Deutschland noch stärker für das Thema IT-Sicherheit zu sensibilisieren.

Die Vereinbarung sieht unter anderem den gegenseitigen Austausch exklusiver Inhalte sowie die Beratung durch NIFIS-Experten im Rahmen des COMPUTERWOCHE Security-Expertenrats vor. Des Weiteren wird NIFIS im Rahmen der Zusammenarbeit Warnhinweise zu den aktuellsten Sicherheitslücken liefern.

„Allein die Erkenntnis und nachfolgende Lippenbekenntnisse reichen nicht aus, um das Niveau der Informations-Sicherheit in Deutschland anzuheben. Der Gesetzgeber ist aufgefordert, in enger Kooperation mit den Mittelstands- und Sicherheitsverbänden verbindliche Vorschriften für die IT-Sicherheit in der Wirtschaft zu entwickeln und durchzusetzen“, fordert Peter Knapp, Vorstandsvorsitzender NIFIS. ❑

NIFIS begrüßt neue Mitglieder

SIEMENS, DEKRA, Völcker Informatik, ConSecur, Datenschutz Management Bovekamp, Nicole Kleff IS-Consulting und Syntlogo sind neue Mitglieder der NIFIS. Wir heißen Sie herzlich willkommen.

Nutzen Sie die Möglichkeit, und gestalten Sie die Aktivitäten unseres Vereins. NIFIS ist für alle Unternehmen und Personen offen, die sich für das Thema Internet-Sicherheit interessieren und versteht sich als Ansprechpartner für Ihre Fragen oder Probleme.

Nicht nur für Großunternehmen ist eine Mitgliedschaft interessant. Besonders kleine und mittelständische Unternehmen profitieren von den Angeboten der NIFIS. ❑

Erste europäische Identity-Management-Konferenz tagt in München

Vom 7. bis zum 10. Mai findet in München die 1st European Identity Conference 2007 statt. In fünf verschiedenen Themenblöcken werden alle wichtigen Aspekte rund um Identity Management, Compliance und Identity Risk Management behandelt.

Die Konferenz ist nach Angaben des Veranstalters Kuppinger Cole + Partner das bedeutendste Event für alle, die sich mit diesen Themen auseinandersetzen. Zahlreiche Anwendervorträge liefern Best Practices aus laufenden und abgeschlossenen Projekten. Neben den Vorträgen, Panels und Roundtables mit intensiven Diskussionsmöglichkeiten gibt es auch eine Ausstellung mit Softwareherstellern und Systemintegratoren.

Anmelden können Sie sich unter http://www.id-conf.com. Als Mitglied der NIFIS erhalten Sie einen **Rabatt in Höhe von zehn Prozent** auf die Teilnahmegebühr. Geben Sie dazu bitte bei der Online-Anmeldung einfach den Code **5052** in das dafür vorgesehene Feld ein. ❑

NIFIS AUF DER CEBIT

Auch Vertreter von NIFIS sind wieder auf der CeBIT in Hannover mit dabei. Informationen zur Initiative erhalten Sie in **Halle 1, Stand F 33** auf dem Magirus Messestand. Bei Gesprächswünschen bitten wir, vorab einen Termin zu vereinbaren. Bei Interesse wenden Sie sich bitte an newsletter@nifis.de.

CeBIT Security World

Die CeBIT Security World ist weiter gewachsen und erstreckt sich auf der CeBIT 2007 vom 15. bis 21. März in den Hallen 6 und 7. Mehr als 250 Aussteller werden auf einer Fläche von 8.500 Quadratmetern ihre Produkte und Lösungen zur IT-Sicherheit präsentieren.

Das Angebotsspektrum reicht von Spam- und Virenschutz über Firewall, Biometrie, Kryptografie, Sicherheitsprüfungen und -zertifizierungen, physische und organisatorische Sicherheitslösungen wie Zugriffsschutz und Zugriffskontrolle bis hin zur Beratung und Planung hochverfügbarer Rechenzentren und Serverparks. ❑

Online-Datensicherung aus verschiedenen Blickwinkeln

Online-Datensicherung aus wirtschaftlicher, technischer und rechtlicher Sicht zu betrachten – diese Möglichkeit bietet Interxion am 28. März in Horb am Neckar. Die Teilnehmer können sich in Vorträgen unverbindlich und kostenlos über diese Backuptechnologie informieren.

Online-Datensicherung ist nicht nur wirtschaftlich und technisch eine interessante Alternative: Der Gesetzgeber verpflichtet das Management von Unternehmen, persönlich für ein Sicherheitssystem zu sorgen, damit Gefahren für Unternehmen frühzeitig erkannt werden können.

Dies bezieht sich speziell auch auf Datensicherung, denn sollten die kritischen und wichtigen Datenbestände eines Unternehmens nicht verfügbar sein, kann schnell eine existenzbedrohende Krise entstehen. In einem solchen Fall können Geschäftsführer, Vorstände und IT-Verantwortliche auch mit ihrem Privatvermögen für den Schaden verantwortlich gemacht werden. Die Agenda und eine Anmeldemöglichkeit gibt es hier. ❑

SAVE THE DATE: Mitgliederkongress und Mitgliederversammlung 2007

Alle Vereinsmitglieder sind herzlich zur Mitgliederversammlung der NIFIS eingeladen. Diese findet am 22. Mai in Frankfurt am Main statt.

Bereits am Morgen treffen sich Mitglieder und Interessenten, um sich im Rahmen eines Kongresses über die neuesten Entwicklungen im Bereich Internet-Sicherheit zu informieren.

Am Nachmittag folgt dann die eigentliche Mitgliederversammlung, die anschließend durch ein nettes Get Together abgerundet wird. Die offizielle Einladung und die Tagesordnung werden den Mitgliedsunternehmen separat zugestellt.

Wir über uns

Mitgliederinterview Claranet

Als NIFIS-Gründungsmitglied gibt Claranet Einblick in die sichere IP-Kommunikation in Unternehmensnetzwerken

clara.net
Internet Service Provider

Die Claranet GmbH hat sich seit ihrer Gründung 1996 zum größten unabhängigen Non-Telco-Service-Provider für Geschäftskunden in Europa entwickelt. Sie bietet ein umfassendes Lösungsportfolio im Bereich Internet Access, Business Hosting, IP-Telefonie, Virtual Private Networks (VPN) und Security Solutions. Das inhabergeführte Unternehmen beschäftigt derzeit deutschlandweit 100, europaweit über 600 Mitarbeiter und bietet mehr als 180.000 Geschäftskunden Internet Services an.

Die Redaktion von NIFIS advice sprach mit

Tarkan Akman
Marketing Director

Uli Schunk
Marketing Executive

Sie sind Gründungsmitglied von NIFIS. Warum unterstützen Sie die Initiative?

Akman: Wir haben gemeinsam mit den anderen Gründungsmitgliedern überlegt: Wie können wir helfen, kaum beachtete Sicherheitsrisiken im IT-Umfeld bekannter zu machen? Wir haben uns entschieden, dass wir uns bei diesem wichtigen Thema nicht auf andere verlassen wollen und gründeten eine eigene Initiative. Aus der Wirtschaft für die Wirtschaft. NIFIS ist eine tolle Idee, um Unternehmen Möglichkeiten zur IT-Sicherheit aufzuzeigen, die nicht unbedingt teuer sein müssen, aber effektiv sind. Wir als Claranet möchten unser Know-how im IP-Umfeld einbringen. Gerade im Bereich der Unternehmensvernetzung sehen wir viele Sicherheitslücken und können hier umfassend beraten.

Was sind das denn für Sicherheitslücken?

Akman: Zum Beispiel kann das Netzwerk nicht sicher verschlossen sein. Das Unternehmen verwendet vielleicht eine Firewall, hat sich aber keine Gedanken gemacht, wie diese effektiv verwaltet wird. Ist das Firewall-Management optimal? Werden Verschlüsselungstechnologien eingesetzt? All das muss bedacht werden, und viele IT-Leiter benötigen gerade hier Beratung.

IP-Kommunikation: Für welche Unternehmen ist das überhaupt interessant?

Akman: Für jedes Unternehmen, das in irgendeiner Weise Kommunikation über das Internet Protocol betreibt. Sei es das Ein-Mann-Unternehmen oder der Großkonzern – im Bereich der IP-Kommunikation kommen sie zwangsläufig zum Thema IP-Sicherheit. E-Mails sind aus der heutigen Geschäftswelt kaum mehr wegzudenken, Internet-Telefonie wird immer beliebter, Außendienstmitarbeiter greifen von unterwegs auf Firmenserver oder interne Datenbanken zu. Kurzum: Jedes Unternehmen muss sich über IP-Sicherheit Gedanken machen.

Warum wird so vieles auf IP-Kommunikation umgestellt?

Schunk: Die Bedeutung von IP-Kommunikation nimmt zu, weil Unternehmen mehr und mehr mit neuen Herausforderungen konfrontiert werden. Ich sage nur: Globalisierung, zunehmender Wettbewerb, steigender Kostendruck. All das zwingt sie, sich auf ihre eigentlichen Kernkompetenzen zu konzentrieren, um erfolgreich am Markt bestehen zu können. IP-Kommunikation fördert die Zusammenführung der Sprach- und Datenkommunikation bei maximaler Ausnutzung der vorhandenen Infrastruktur. Eventuell vorhandene Doppel-Infrastrukturen werden hinfällig. Dabei sind wesentliche Erfolgsfaktoren in der Welt der IP-Kommunikation, neben breitbandigen Internet-Zugängen, besonders zuverlässige und effektive Verschlüsselungsmechanismen.

Inwiefern ist ein kleines Unternehmen denn gefährdet?

Akman: Ein Virus unterscheidet an der IP-Adresse nicht, ob es ein kleines oder großes Unternehmen ist. Das Netzwerk wird befallen und mit jeder E-Mail, die rausgeht, sind weitere Unternehmen betroffen. Auch Hacker sind eine Gefahr, weil sie immer häufiger Robots für Unternehmensangriffe nutzen, die nicht zwischen klein und groß unterscheiden.

Firewall und Virenscanner haben aber mittlerweile viele Unternehmen. Was sind im Bereich der der IP-Kommunikation die häufigsten Sicherheitslücken?

Akman: Software und Hardware werden nicht optimal genutzt beziehungsweise nicht ausführlich und gewissenhaft gemanagt. Dadurch entstehen Sicherheitslücken. Es ist nicht damit getan, zu sagen: „Ich habe jetzt eine Firewall, die stell' ich mir da hin, und ich habe eine Software, die schützt mich vor Viren"; ich muss das Ganze auch aktiv managen, Updates durchführen, die Ports vernünftig verwalten usw. Bestes Wissen und Gewissen reichen meist nicht aus. Hier sollte man auf die Fachkompetenz von Spezialisten wie NIFIS zurückgreifen. ►

Schunk: Mit Virenscannern allein ist es in den meisten Fällen nicht getan. Allzu oft wird auch die Sicherheit im eigenen LAN vernachlässigt. Dem kann man mit einer Verschlüsselung mittels eines VPNs entgegensteuern. Je nach Vorgabe kann die Zugangsberechtigung für bestimmte Daten auf die entsprechende Benutzergruppe beschränkt werden. Damit ist die Gefahr der „Betriebsspionage" von innen heraus gebannt.

Wie gehen Sie vor, wenn Sie ein Unternehmen in dem Bereich um Hilfe bittet?

Schunk: Unser Ziel ist es, unseren Kunden von der Konzeption über die Realisierung bis zum Betrieb im Alltag jederzeit leistungsfähige und kompetent betriebene IP-Services zu bieten. Um dieser Anforderung gerecht zu werden, stehen unsere IT-Consultants den Unternehmen beratend zur Seite, analysieren die Infrastruktur vor Ort, erarbeiten Sonderlösungen und beraten die Interessenten in technischen Fragen.

Und wie unterstützen Sie gezielt NIFIS-Mitglieder bei der Sicherung der IP-Kommunikation?

Akman: Wir stellen den Mitgliedern kostenfrei unser spamVir protect zur Verfügung. Die leistungsfähige Kombi-Lösung aus Spam-Filter und Virenscanner schützt E-Mail-Accounts vor Viren und unerwünschten Spam-Mails. Darüber hinaus unterstützen wir in den Arbeitskreisen die NIFIS-Mitglieder mit unserem Know-how und informieren die Wirtschaft auf Veranstaltungen aktiv über Internet-Sicherheit und sichere IP-Kommunikation.

Schunk: Ich selbst habe als Claranet-Vertreter unter anderem in einem Arbeitskreis das NIFIS-Siegel mit entwickelt. Die Unternehmen führen hierbei einen umfangreichen Selbst-Audit durch, der sich an der Norm ISO/IEC 27001 (BS7799) orientiert, um pragmatisch und einfach ihren Sicherheitsstandard zu überprüfen. Der NIFIS-Siegelrat, dem ich auch angehöre, wertet dann die Antworten aus. Bei einer positiven Bewertung erhält ein Unternehmen für den Zeitraum von zwölf Monaten das NIFIS-Siegel. Außerdem wird ein Ergebnisprotokoll ausgestellt, das eventuell vorhandene Sicherheitslücken oder Schwachstellen explizit ausweist. Somit hat das Unternehmen konkrete Anhaltspunkte für mögliche Verbesserungen seiner Internet-Sicherheit.

Warum sollten weitere Unternehmen Mitglied bei NIFIS werden?

Akman: Mitglieder bekommen zahlreiche interessante Angebote und Vergünstigungen, beispielsweise spamVir protect von Claranet. Außerdem können sie das NIFIS-Siegel kostenfrei beantragen – Nicht-Mitglieder zahlen dagegen 150 Euro. Ganz wichtig ist auch, dass sie von dem Know-how der anderen Mitglieder profitieren, indem sie etwa an Arbeitskreisen teilnehmen. Sie erhalten Informationen schnell und aus erster Hand. Bei NIFIS sind IT-Experten aus verschiedenen Branchen vertreten. Diese interdisziplinäre Zusammensetzung und der direkte Zugang zu neutralen Informationen bringen den NIFIS-Mitgliedern einen entscheidenden Wettbewerbsvorteil.

Wie sehen Sie die weitere Entwicklung von NIFIS?

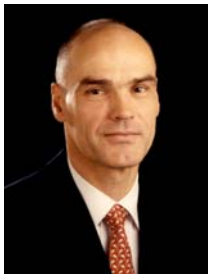
Akman: In der relativ kurzen Zeit, in der wir mit NIFIS aktiv sind, haben wir sehr viel positive Resonanz erfahren – sowohl in Fachkreisen als auch in der Presse. Aber wir müssen weiter an unserer Positionierung arbeiten. Ich bin überzeugt, wir werden viele neue Mitglieder gewinnen, denn das Thema Internet-Sicherheit und vor allem auch das Feld IP-Sicherheit, das Kompetenzthema der Claranet, ist für die Zukunft in Bezug auf Konvergenz von Sprache und Daten enorm wichtig. Mein Wunsch wäre, dass jeder IT-Verantwortliche NIFIS kennen und als Informationsforum schätzen lernt.

Wir danken für dieses Gespräch! ❑

Service

Identity Management = wichtige unternehmensorganisatorische Aufgabe

Wie bereits in NIFIS advice 04/2006 berichtet, hat NIFIS ein Kompetenzzentrum zu „Identity Management" gegründet. Es befasst sich mit Fragen, Problemen und konkreten Lösungen im Zusammenhang mit der ganzheitlichen Verwaltung digitaler Identitäten. Den Vorsitz des neuen Expertenforums hat Dr. Horst Walther, Partner bei Kuppinger Cole + Partner, übernommen. Er schildert in der heutigen Ausgabe, warum das Thema so wichtig ist, wer dem Kompetenzzentrum angehört, und welche Ziele es anstrebt.

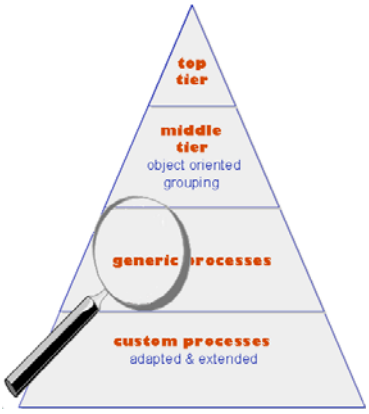


Dr. Horst Walther

Es gibt wohl nur wenige Aufgaben im Informations-Sicherheitsmanagement von Unternehmen, die nicht mit der Identität von Personen und deren Beziehung zu den sicherheitsrelevanten Unternehmensobjekten zu tun haben. Das macht das Identity- und Access Management (IAM) für alle, die sich mit IT-Sicherheit befassen, zu einem wichtigen Thema. Dennoch ist IAM nicht als Untermenge der IT-Sicherheit zu betrachten. Es stellt vielmehr eine eigenständige Infrastrukturdisziplin dar. IAM ist eher als zentrale und unternehmensweit wahrzunehmende Organisationsaufgabe einzustufen. Es ist damit auch ein wichtiges Thema für NIFIS. So war es nur folgerichtig, dass sich am 1. Dezember des vergangenen Jahres am Rande der Digital ID World in Wiesbaden das Kompetenzzentrum „Identity Management" konstituiert hat. Zu den Gründungsmitgliedern gehören namhafte DAX-Unternehmen wie Siemens oder BMW von der Anwenderseite, große Hersteller von IAM-Lösungen wie Novell, ORACLE, Siemens oder SUN, eine Reihe von Beratungshäusern und Systemintegratoren ►

sowie das Analystenhaus Kuppinger Cole + Partner. Wir sehen IAM als unternehmensorganisatorische Aufgabe. Es hat jedoch eine starke technische Komponente. Zum einen hat die gestiegene Komplexität der zu verwaltenden Berechtigungen für den Zugriff auf IT-Systeme einen gewissen Leidensdruck entstehen lassen. Dieser wird noch verstärkt durch die Notwendigkeit, die Compliance zu bestimmten gesetzlichen Regelungen nachzuweisen. Zum anderen lässt sich diese Aufgabe erst durch den Einsatz spezialisierter Verwaltungs- und Reportingsysteme lösen. Das Kompetenzzentrum Identity Management will sich daher mit den beiden kritischen Schnittstellen zwischen Organisation und Technik befassen: den IAM-Prozessen und den Mitarbeiterrollen.

Baukasten für Identity- und Access Management



Die Aktivitäten zum Thema Prozesse sind bereits unter dem Motto „GenericIAM – generische Prozesse für das Identity- und Access Management“ angelaufen. Hier haben wir uns zum Ziel gesetzt, einen Baukasten typischer, in den Unternehmen immer wieder auftauchender, „generischer“ Prozesse für das Identity- und Access Management zusammenzustellen. Mit diesem Referenzmodell soll es künftig den Unternehmen möglich sein, IAM-Projekte mit deutlich reduziertem Aufwand zum Erfolg zu führen. Es ist schlicht nicht einzusehen, warum jedes Unternehmen immer wieder mit „einem weißen Blatt Papier“ beginnt und alle IAM-Prozesse neu „erfindet“. Sie enthalten schließlich einen großen Kern von Prozessen, die für viele Unternehmen gleich sind.

Eine Mitwirkung an diesem Vorhaben ist für alle Marktteilnehmer sinnvoll. Anwenderunternehmen werden allerdings den größten Nutzen haben. Sie können so bestehende Lücken füllen, ihre Prozesse optimieren und Kosten senken. Durch Aufsetzen auf einem standardisierten und harmonisierten Modell erhalten sie eine höhere Sicherheit, auch (zukunfts-) sichere, optimierte Prozesse einzusetzen, die sich an den Best-Practice-Beispielen der gesamten Disziplin orientieren. Integratoren und Systemanbieter, freiberufliche Projektleiter und Berater können bereits umfangreiche und wirklichkeitsnahe Musterprozesse mitliefern und so für ihre Kunden messbaren Mehrwert schaffen. Insgesamt soll GenericIAM durch das Bereitstellen eines allgemein anerkannten und verwendeten Referenzmodells zur Reifung des Identity- und Access Managements beitragen.

Wenn Sie sich aktiv an der Entwicklung des generischen IAM-Modells beteiligen möchten, dann senden Sie bitte eine E-Mail an Herrn Dr. Walther, den Leiter des Expertenforums. ❑

Praxistipp

Identity- und Access Management zum Schutz von Informationswerten


Brad Chapman
Vorstand NIFIS

In allen Unternehmen spielen Daten und Informationen eine immer wichtigere Rolle, in einigen stellen sie bereits den wichtigsten Wert dar. Diese Informationen sind einer Vielzahl von Risiken ausgesetzt, und ihr Schutz stellt für viele Unternehmen eine komplexe Herausforderung dar.

Immer mehr und unterschiedliche Gruppen von Personen, wie zum Beispiel eigene und externe Mitarbeiter, Partner, Zulieferer und Kunden, greifen – zum Teil über das Internet – auf Informationen zu. Die nachvollziehbare und effiziente Verwaltung der Identitäten und ihrer Zugriffsrechte ist somit die zentrale Komponente zum Schutz der Informationswerte!

Folgende Fragestellungen können helfen, um eine erste Selbsteinschätzung hinsichtlich der Frage vorzunehmen, ob der Schutz in einem ausreichenden Maße umgesetzt wurde:

1. Kann auf jedem System / in jeder Anwendung jedes Benutzerkonto eindeutig einer Person zugeordnet werden?
2. Wird die Einrichtung neuer Benutzerkonten und Berechtigungen für Personen für jedes System / jede Anwendung nachvollziehbar dokumentiert und durch den jeweiligen System- / Dateneigentümer genehmigt?
3. Werden die nicht mehr notwendigen Benutzerkonten und Zugriffsrechte bei Austritt oder Aufgaben- / Abteilungswechsel einer Person auf allen Systemen / in allen Anwendungen zeitnah gesperrt beziehungsweise entzogen? Gilt dies auch für externe Benutzer?
4. Besteht ein Überblick über alle Personen, deren Benutzerkonten und Berechtigungen?
5. Erfolgt regelmäßig eine Überprüfung durch das Business, ob die aktuell vergebenen Berechtigungen für alle Personen korrekt sind?
6. Sind verbotene Kombinationen von Berechtigungen (Segregation of Duties) definiert, und wird deren Einhaltung sichergestellt und überprüft? ►

7. Sind umfassende administrative Berechtigungen auf Notfalluser beziehungsweise wenige Personen beschränkt, und werden die Aktivitäten dieser Benutzerkonten (datenschutzgerecht) protokolliert und regelmäßig ausgewertet?
8. Werden alle sicherheitskritischen Ereignisse protokolliert und regelmäßig ausgewertet?

Entsprechende Prozesse und Maßnahmen sollten Teil des internen Kontrollsystems eines Unternehmens sein, um regulatorische Anforderungen und unternehmensindividuelle Sicherheitsbedürfnisse erfüllen zu können. Software-Tools können grundsätzlich bei der effektiven Umsetzung von Prozessen und Kontrollen unterstützen. Vorab ist jedoch immer die individuelle Definition der Richtlinien sowie der Prozesse und Kontrollen notwendig.

Bei Rückfragen wenden Sie sich bitte an newsletter@nifis.de. ❑

Sicherheitsupdate

PDAs: Sensible Datenträger

Neun von zehn Geschäftsleuten speichern vertrauliche Geschäftsinformationen auf mobilen Endgeräten wie Smartphones oder PDAs. Das ermittelte Dynamic Markets in einer Befragung von 500 europäischen Unternehmen. Gesichert werden die Daten bei drei Viertel mit Passwortabfrage. Jedem fünften Unternehmer ist allerdings schon einmal das mobile Gerät abhanden gekommen.

Rund 97 Prozent der deutschen Geschäftsleute speichern sensible Daten auf mobilen Endgeräten. Sie haben europaweit die größten Bedenken (fast 70 Prozent) über deren Sicherheit geäußert. Knapp 60 Prozent der Deutschen schützen ihre wichtigen Unternehmensinformationen, indem sie ihr Gerät niemand anderem anvertrauen, jeder Zehnte ergreift keinerlei Maßnahmen. ❑

Sicherheitslücke Raucher

Raucher können die IT-Sicherheit gefährden. Das ermittelte das britische Security-Unternehmen NTA Monitor in einem Test. Rauchfreie Zonen oder Gebäude treiben die Raucher zunehmend ins Freie. Dort könnten sie zum Sicherheitsleck werden, indem sie nach der Zigarettenpause Türen offen lassen. Ein NTA-Tester konnte aufgrund der Nachlässigkeit ins Gebäude gelangen und in einem Konferenzraum sein Notebook an das firmeneigene VoIP-Netz anschließen. Theoretisch hätte er auf diese Weise eine Denial-of-Service-Attacke (DoS) starten oder Telefongespräche abhören können. ❑

IMMER UP TO DATE

Um Sie effizient zu schützen, bietet NIFIS auf ihrer Website tagesaktuelle Warnhinweise zu Bedrohungen im Internet. Alle aufgeführten Meldungen sind CERT-geprüft (Computer Emergency Response Team) und haben ein hohes Schadens- und Risikopotenzial. Links zu weiterführenden Informationen unterstützen Sie beim schnellen Beseitigen der Sicherheitsbedrohung.

Sicherheitsforschung

Das Bundeskabinett hat ein ressortübergreifendes Programm zur Sicherheitsforschung beschlossen. In der ersten Förderperiode von 2007 bis 2010 will die Bundesregierung hierfür Haushaltsmittel von rund 123 Millionen Euro bereitstellen.

Das Förderprogramm besteht aus zwei Programmlinien. Die erste umfasst die „Szenarienorientierte Sicherheitsforschung". Programmlinie 2 zielt auf die Erforschung von Querschnittstechnologien in „Technologieverbünden" ab. Dazu zählen unter anderem die Technologien zur schnellen und sicheren Personenidentifikation. Erste Ausschreibungen sollen bereits im März erfolgen.

Das Förderprogramm ist integrierter Teil der Hightech-Strategie der Bundesregierung und soll eine spezielle Plattform bieten, auf der Industrie, Forschungseinrichtungen und Hochschulen mit Behörden, Rettungs- und Sicherheitsdiensten sowie den Betreibern kritischer Infrastrukturen zusammenarbeiten können. ❑

2006: Verwundbare Web-Anwendungen treiben Zahl der Schwachstellen in die Höhe

Nach den Statistiken des CERT/CC (Computer Emergency Response Team Coordination Center) ist die Zahl der 2006 gemeldeten Schwachstellen bereits das zweite Jahr in Folge sprunghaft gestiegen.

Nach Informationen des von der US-amerikanischen Carnegie Mellon University betriebenen CERT/CC ist die Zahl der gemeldeten Sicherheitslücken im vergangenen Jahr von 5.990 auf 8.064 Lecks gestiegen. Den Experten zufolge waren in erster Linie Fehler in Web-Applikationen für den Zuwachs an Schwachstellen (plus 35 Prozent) verantwortlich.

Bug-Zuwächse zwischen 20 und 35 Prozent verzeichneten laut einem Bericht von Security Focus auch andere Schwachstellendatenbanken wie die National Vulnerability Database (NVD), die Open-Source Vulnerability Database (OSVDB) und Symantecs Vulnerability Database. So sollen laut Symantec bereits in der ersten Hälfte 2006 mehr als drei Viertel aller Softwarefehler Online-Anwendungen betroffen haben.

Auch nach einem im Oktober veröffentlichten Report des Common Vulnerabilities and Exposures (CVE) Project haben Sicherheitslecks in Web-Programmen in den ersten neun Monaten des Jahres 2006 rund 45 Prozent aller Schwachstellen ausgemacht.

Diesen Trend führen die CERT-Experten nicht zuletzt darauf ►

zurück, dass es etwa mittels Source-Code-Checks immer leichter wird, Schwachstellen in Online-Anwendungen aufzuspüren. Zudem stellten die betroffenen Applikationen, die häufig in kleinen Firmen oder von Einzelpersonen eingesetzt würden, nicht zwingend eine direkte Bedrohung für Unternehmen dar.

(Katharina Friedmann, Redaktion COMPUTERWOCHE)

Weitere aktuelle Security-Informationen finden Sie hier. ❑

IMPRESSUM

Herausgeber
NIFIS e.V.
Weismüllerstraße 21
60314 Frankfurt
Tel.: 0 69 / 40 80 93 70
Fax: 0 69 / 40 14 71 59
E-Mail: newsletter@nifis.de
Internet: http://www.nifis.de
Peter Knapp (V.i.S.d.P.)

Redaktion
FRESH INFO +++
http://www.fresh-info.de